**EMERGING TECHNOLOGY LEGISLATION**

In the 116th and 117th sessions of Congress, hundreds of pieces of legislation have proposed various ways to address issues raised by emerging technologies. The bills listed in this appendix offer a representative sampling of the proposals dealing with artificial intelligence, biotechnology, and cybersecurity. In each case, descriptive paragraphs and complete texts of the legislation are available at www.congress.gov. None of the bills listed below actually become public law, meaning that each one could become a prototype for an affirmative case on the 2022-23 emerging technology topic.

*Advancing American AI Act;* S.1353 117th Congress; Sponsor: Sen. Peters, Gary C. [DMI]: This bill requires specified federal agencies to take steps to promote artificial intelligence (AI) while aligning with U.S. values, such as the protection of privacy, civil rights, and civil liberties. The Office of Management and Budget must establish mechanisms to continually refine guidance issued to agencies regarding AI as best practices evolve, issue a memorandum to each agency that articulates the method by which the agency shall make public information about the agency’s use of AI, and identify at least five new use cases for the application of cross-enterprise AI-enabled systems to support modernization initiatives across agencies.

*Advancing American Artificial Intelligence Innovation Act of 2021;* S.3175 117th Congress; Sen. Rosen, Jacky [D-NV]: This bill requires the Department of Defense (DOD) to implement a pilot program to assess the feasibility and advisability of establishing data libraries for developing and enhancing artificial intelligence capabilities to ensure that DOD is able to procure optimal artificial intelligence and machine learning software capabilities. DOD must brief the congressional defense committees on the implementation of this pilot program.

*Advancing Cybersecurity Diagnostics and Mitigation Act;* S.2318 116th Congress; Sponsor: Sen. Cornyn, John [R-TX]: This bill requires the Department of Homeland Security (DHS) to establish a program to assist agencies with continuously diagnosing and mitigating cyber threats and vulnerabilities. Pursuant to this program, DHS shall (1) develop the capability to collect, analyze, and visualize information relating to security data and cybersecurity risks at agencies; (2) make program capabilities available for use by civilian agencies, states, and local governments; (3) assist such entities in setting information security priorities and assessing and managing cybersecurity risks; and (4) develop policies and procedures for reporting systemic risks and potential incidents. DHS must also regularly deploy new technologies to improve the program. In addition, the Government Accountability Office must report on the potential impacts and benefits of replacing existing reporting requirements under the federal information policy with periodical real-time data provided by the program.

*AI in Counterterrorism Oversight Enhancement Act;* H.R.4469 117th Congress; Sponsor: Rep. Maloney, Carolyn B. [D-NY-12]: This bill expands the responsibilities of the Privacy and Civil Liberties Oversight Board to include oversight of the use of artificial intelligence (AI) in counterterrorism and addresses related issues. Specifically, the board must continually review any AI-enabled technologies used in counterterrorism efforts and determine whether such technologies protect privacy and civil liberties and adhere to relevant policies. The bill also expands the board’s authorities to access or subpoena information to include information about AI-enabled technologies used for counterintelligence, such as the training and testing processes for such technologies. Furthermore, the bill expands the responsibilities of privacy and civil liberties officers to include responsibilities related to AI-enabled technologies used in counterterrorism. (Currently, the statute requires certain departments and agencies, including the Department of Justice and the Office of the Director of National Intelligence, to each designate one senior officer as a privacy and civil liberties officer to provide certain information to the board.)

*Artificial Intelligence for Agency Impact Act or the AI for Agency Impact Act;* H.R.4468 117th Congress; Rep. Maloney, Carolyn B. [D-NY-12]: This bill requires each federal agency to establish and implement an artificial intelligence (AI) strategy, objectives, and metrics plan. Each plan shall include defined roles, responsibilities, and delegation of authority for AI use and oversight; defined values, ethics, and principles to foster public trust and responsible use of AI; procedures to ensure data security and privacy and for human supervision and accountability; performance objectives and accompanying metrics that clearly reflect or convey the intended purpose of the AI; documentation demonstrating that the AI relies on high quality, reliable, representative data; a description of how the AI is monitored; and a description of how information on the design, operation, limitations, and updates of the AI is made available to the public.

*Artificial Intelligence for the Military Act of 2021;* S.1776 117th Congress; Sen. Portman, Rob [R-OH]: This bill requires the implementation of training and education related to emerging technologies and artificial intelligence for certain military personnel. The bill requires expansion of the curriculum for military junior leader education to incorporate training material related to focuses that include problem definition and curation and a conceptual understanding of the artificial intelligence life cycle. Such training and education should include the use of existing artificial intelligence-enabled systems and tools. The Department of Defense (DOD) must ensure that the curriculum for professional military education is revised in each of the military services to incorporate periodic courses on militarily significant emerging technologies. DOD must establish a short course on emerging technologies for general and flag officers and senior executive-level civilian leaders. The course must be taught on an iterative, two-year cycle and address the most recent and relevant technologies and the application of these technologies to military and business outcomes in DOD.

*Artificial Intelligence Standards and National Security Act;* S.4082 116th Congress; Sponsor: Sen. Bennet, Michael F. [D-CO]: This bill requires the Department of Defense (DOD) to submit certain reports with respect to artificial intelligence. Specifically, DOD must report to Congress on the role of DOD in the development of artificial intelligence standards, including an assessment of the ways in which an artificial intelligence standards strategy will improve the national security; and the feasibility and current status of assigning members of the Armed Forces on active duty to the Joint Artificial Intelligence Center of DOD.

*Artificial Intelligence Training for the Acquisition Workforce Act or the AI Training Act;* S.2551 117th Congress; Sponsor: Sen. Peters, Gary C. [D-MI]: This bill requires the Office of Management and Budget (OMB) to establish or otherwise provide an artificial intelligence (AI) training program for the acquisition workforce of executive agencies (e.g., those responsible for program management or logistics), with exceptions. The purpose of the program is to ensure that the workforce has knowledge of the capabilities and risks associated with AI. The OMB must (1) update the program at least every two years, and (2) ensure there is a way to understand and measure the participation of the workforce and to receive and consider feedback from program participants.

*Assessing a Cyber State of Distress Act of 2020;* S.4226 116th Congress; Sponsor: Sen. Peters, Gary C. [D-MI]: This bill requires the Department of Homeland Security (DHS) to assess the feasibility and advisability of establishing (1) an authority for the declaration of a cyber state of distress, and (2) a Cyber Response and Recovery Fund. Both required assessments shall include a review of recommendations by the Cyberspace Solarium Commission established to develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences. Further, the assessment of an authority for declaring a cyber state of distress shall include the development of additional recommendations relating to (1) any determinations that DHS should make and other actions that should be taken before DHS is authorized to declare or renew a cyber state of distress, (2) the definition of the term significant cyber incident, and (3) the appropriate duration of a cyber state of distress. The assessment of a Cyber Response and Recovery Fund shall include the development of additional recommendations relating to (1) the administration of such a fund, (2) the eligibility of entities that may receive support from such fund, and (3) allowable expenses for such fund. DHS must provide a briefing that includes findings from each assessment and legislative proposals for the establishment of an authority for the declaration of a cyber state of distress and a Cyber Response and Recovery Fund.

*Better Cybercrime Metrics Act;* H.R.4977 117th Congress; Sponsor: Rep. Spanberger, Abigail Davis [D-VA-7]: This bill establishes various requirements to improve the collection of data related to cybercrime and cyber-enabled crime (cybercrime). Among the requirements the Department of Justice (DOJ) must enter into an agreement with the National Academy of Sciences to develop a taxonomy for categorizing different types of cybercrime faced by individuals and businesses; DOJ must establish a category in the National Incident-Based Reporting System for collecting cybercrime reports from federal, state, and local officials; DOJ’s Bureau of Justice Statistics and the Bureau of the Census must include questions about cybercrime in the annual National Crime Victimization Survey; and the Government Accountability Office must assess the effectiveness of reporting mechanisms for cybercrime and disparities in reporting cybercrime data and other types of crime data.

*Cyber Defense National Guard Act;* H.R.119 117th Congress; Sponsor: Rep. Jackson Lee, Sheila [D-TX-18]: This bill requires the Office of the Director of National Intelligence to report to Congress regarding the feasibility of establishing a Cyber Defense National Guard. The report shall address topics including (1) the cost of creating a Cyber Defense National Guard, (2) the number of persons needed to defend critical U.S. infrastructure from a cyberattack, (3) the sources of potential members of the Cyber Defense National Guard, and (4) which federal government elements would be best equipped to train and manage the Cyber Defense National Guard.

*Cyber Diplomacy Act of 2021;* H.R.1251 117th Congress; Sponsor: Rep. McCaul, Michael T. [R-TX-10]: This bill establishes requirements related to diplomatic engagement with foreign countries on matters of U.S. cyberspace policy. Specifically, the bill establishes the Bureau of International Cyberspace Policy within the Department of State to advise the State Department on cyberspace issues and lead diplomatic efforts on issues related to international cybersecurity, internet access and freedom, and international cyber threats. The bureau must undertake specified duties and responsibilities to implement the stated U.S. policy of working internationally to promote an open, interoperable, and secure internet governed by a multi-stakeholder model that (1) promotes human rights, democracy, and rule of law; and (2) respects privacy and guards against deception, fraud, and theft. The President must devise a strategy for U.S. engagement with foreign governments on international norms related to responsible state behavior in cyberspace. Further, the President is encouraged to enter into executive arrangements with foreign governments that support U.S. cyberspace policy. In addition, annual country reports on human rights practices must include assessments of freedom of expression in each country with respect to electronic information, and the Government Accountability Office must report on U.S. diplomatic processes and other efforts with foreign countries to advance U.S. interests in cyberspace.

*Cyber Essentials Act;* H.R.8223 116th Congress; Sponsor: Rep. Katko, John [R-NY-24]: This bill requires the Cybersecurity and Infrastructure Security Agency to develop, publish, and maintain evidence-based guidelines and processes that individuals can follow to defend against common cybersecurity threats and risks.

*Cyber Incident Notification Act of 2021;* S.2407 117th Congress; Sponsor: Sen. Warner, Mark R. [D-VA]: This bill requires federal agencies and certain entities to report cybersecurity intrusion incidents to the Cybersecurity and Infrastructure Security Agency (CISA) and addresses related issues. Within 24 hours of a confirmed intrusion (or potential intrusion), the targeted agency or entity must report the intrusion to CISA. CISA must promulgate rules relating to the bill, including the information that must be included in each incident report and the entities that must comply with the reporting requirements. At minimum, the covered entities must include federal contractors and owners or operators of critical infrastructure. Similarly, such rules must at minimum require federal agencies and covered entities to report all intrusions involving a nation-state, advanced persistent threat cyber actor, or transnational organized crime group. If a covered entity fails to meet the bill’s requirements, CISA may assess a civil penalty of up to 0.5% of the entity’s gross revenue for each day the violation lasts. If the violating entity has federal contracts, the General Services Administration may impose additional penalties, including removal from the Federal Contracting Schedule.

*Cyber Leap Act of 2020;* S.3712 116th Congress; Sen. Wicker, Roger F. [R-MS]: This bill requires the Department of Commerce to establish national cybersecurity grand challenges to achieve high-priority breakthroughs in cybersecurity. These challenges will offer cash and noncash prizes to winners and shall include competitions that encompass building more resilient systems that raise adversary costs of carrying out common cyberattacks, empowering people with a sufficient level of digital literacy to make safe and secure decisions online and developing a cybersecurity workforce to protect and maintain information systems, advancing cybersecurity efforts in response to emerging technologies, maintaining usability while improving the security and safety of individuals’ online activity, and reducing cybersecurity risks to federal networks and systems and improving the response of federal agencies to cybersecurity incidents. Commerce must designate an advisory council to seek recommendations for the scope of the challenges and for metrics to assess submissions for prizes.

*Cyber Response and Recovery Act of 2021;* S.1316 117th Congress; Sponsor: Sen. Peters, Gary C. [D-MI]: This bill authorizes the Department of Homeland Security (DHS) to declare a significant incident in the event of a breach of a public or private network and establishes a Cyber Response and Recovery Fund. Specifically, DHS may make the declaration upon determining that a specific significant incident has occurred or is likely to occur imminently and that otherwise available resources, other than the fund, are likely insufficient to respond to or mitigate the incident effectively. Upon a declaration, the Cybersecurity and Infrastructure Security Agency must coordinate (1) the response activities of each federal agency; and (2) with other responding entities, including local governments and law enforcement agencies.

*Cyber Sense Act of 2021;* H.R.2928 117th Congress; Sponsor: Rep. Latta, Robert E. [ROH-5]: This bill requires the Department of Energy to establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system. The bulk-power system includes facilities and control systems necessary for operating an interconnected electric energy transmission network.

*Cyber Shield Act of 2021;* H.R.2236 117th Congress; Sponsor: Rep. Lieu, Ted [D-CA-33]: This bill requires the Department of Commerce to establish the Cyber Shield Program, a voluntary program to identify and certify covered products. These products are consumer-facing physical objects that meet industry-leading cybersecurity and data security benchmarks and that can (1) connect to the internet; and (2) collect, send, or receive data or control the actions of a physical object or system. Commerce must also establish a Cyber Shield Advisory Committee to recommend (1) the format and content of Cyber Shield labels for covered products; and (2) the process to identify, establish, report on, adopt, maintain, and promote compliance with industry-leading cybersecurity and data security benchmarks to enhance cybersecurity and protect data. On its website, Commerce must make publicly available (1) program information, (2) a database of covered products certified under the program, and (3) contact information for each manufacturer of a covered product certified under the program.

*Cybersecurity Standards for Aircraft to Improve Resilience Act of 2019 or the Cyber AIR Act;* S.2181 116th Congress; Sponsor: Sen. Markey, Edward J. [D-MA]: This bill addresses cyberattacks on aircraft systems and cybersecurity vulnerabilities to the U.S. commercial aviation system. The Department of Transportation (DOT) must implement regulations to require domestic or foreign air carriers and manufacturers to disclose to the Federal Aviation Administration any attempted or successful cyberattack against any system on board an aircraft or against any maintenance or ground support system for aircraft. DOT must also incorporate cybersecurity into the requirements for obtaining an air carrier operating certificate or a production certificate. The Commercial Aviation Communications Safety and Security Leadership Group must (1) evaluate the cybersecurity vulnerabilities of broadband wireless communications equipment designed for consumer use on board aircraft; and (2) require the implementation by air carriers, manufacturers, and communications service providers of security measures it deems necessary to prevent cyberattacks that exploit such equipment.

*Deepfake Task Force Act;* S.2559 117th Congress; Sponsor: Sen. Portman, Rob [R-OH]: This bill requires the Department of Homeland Security to coordinate with the White House Office of Science and Technology Policy to temporarily establish the National Deepfake Provenance Task Force. Comprised of federal and nonfederal stakeholders, the task force must address threats posed by digital content forgeries (i.e., digital audio, images, and text fabricated or manipulated using artificial intelligence, machine learning, and other emerging technologies with the intent to mislead). The task force’s activities include developing a plan to reduce the proliferation of digital content forgeries.

*Defend COVID Research from Hackers Act;* S.4793 116th Congress; Sponsor: Sen. Tillis, Thomas [R-NC]: This bill authorizes the President to impose visa-blocking, property-blocking, or economic sanctions on a foreign person that is involved in activities that are reasonably likely to result in a significant threat to U.S. national security, foreign policy, public health, economic health, or financial stability. The Department of State must submit a report detailing the extent of known or attempted cyber-enabled activities by foreign persons related to COVID-19 (i.e., coronavirus disease 2019) and assessing whether those activities qualify for the imposition of sanctions.

*Department of Defense Artificial Intelligence Metrics Act of 2021;* S.2904 117th Congress; Sponosor: Sen. Rounds, Mike [R-SD]: This bill requires the Department of Defense (DOD) to review the potential applications of artificial intelligence and digital technology to DOD platforms, processes, and operations. The bill also requires DOD to establish performance objectives and accompanying metrics for the incorporation of artificial intelligence and digital readiness into such platforms, processes, and operations.

*Enhancing K-12 Cybersecurity Act;* H.R.4005 – 117th Congress; Sponsor: Rep. Matsui, Doris O. [D-CA-6]: This bill establishes resources and a program to address cybersecurity of elementary and secondary schools. First, the bill directs the Cybersecurity and Infrastructure Security Agency (CISA) to establish an information exchange to disseminate information, best practices, training, and resources to improve cybersecurity in elementary and secondary schools. In addition, CISA must establish a registry to track cyber incidents affecting information technology systems that are owned or managed by schools and educational agencies. Schools and educational agencies may voluntarily submit information to the registry. Finally, the bill requires CISA to establish a program to address cybersecurity threats to school information systems.

*Federal Cybersecurity Workforce Expansion Act;* H.R.5138 117th Congress; Sponsor: Rep. Houlahan, Chrissy [D-PA-6]: This bill establishes an apprenticeship program and a pilot program on cybersecurity. The Cybersecurity and Infrastructure Agency may establish one or more apprenticeship programs that leads directly to employment in a cybersecurity work role with the agency; or a position with a company or other entity, as prescribed by this bill. The Department of Veterans Affairs (VA) shall establish a pilot program under which the VA shall provide cyber-specific training for members of the Armed Forces transitioning from service in the Armed Forces to civilian life and for veterans.

*Federal Rotational Cyber Workforce Program Act of 2021;* H.R.3599 117th Congres; Sponsor: Rep. Khanna, Ro [D-CA-17] : This bill establishes a rotational cyber workforce program under which certain federal employees may be detailed among rotational cyber workforce positions at other agencies. This bill authorizes an agency to determine whether a workforce position involving information technology, cybersecurity, or other cyber-related functions in that agency is eligible for the program. Additionally, the bill requires the Office of Personnel Management to issue a Federal Rotational Cyber Workforce Program operation plan providing policies, processes, and procedures for detailing employees among rotational cyber workforce positions at agencies. The Government Accountability Office must assess the operation and effectiveness of the rotational cyber workforce program by addressing the extent to which agencies have participated in the program and the experiences of employees serving in the program.

*Future of Artificial Intelligence Act of 2020;* H.R.7559 116th Congress; Sponsor: Rep. Olson, Pete [R-TX-22]: This bill directs the Chief Technology Officer, in the Office of Science and Technology Policy, to establish a Federal Advisory Committee on the Development and Implementation of Artificial Intelligence to advise the President on matters relating to the development of artificial intelligence, including: U.S. competitiveness, including the promotion of investment into the development of artificial intelligence; the U.S. workforce, including the potential for using artificial intelligence for rapid retraining of workers, due to the possible effect of technological displacement; education, including science, technology, engineering, and mathematics education to prepare workers as the needs of employers change; open sharing of data and research on artificial intelligence; international cooperation and competitiveness, including the competitive international landscape for artificial intelligence-related industries; matters relating to individual civil rights, including how rights are or will be affected by the use of artificial intelligence technology and whether such uses should be subject to additional controls, oversight, or limitations; and matters relating to urbanization and the development of smart cities.

*Genome Editing Threat Assessment Act;* H.R.8045 116th Congress; Sponsor: Rep. Joyce, John [R-PA]: This bill requires the Department of Homeland Security (DHS) to develop a threat assessment of the potential homeland security vulnerabilities associated with genome modification and editing. Such assessment shall include information relating to the dual-use of emerging biotechnology; the ability of gene editing to maliciously proliferate infectious diseases and pandemics on human, animal, and plant populations; the cybersecurity vulnerabilities in computer systems analyzing genomic data; and privacy concerns associated with analyzing genomic data. Upon completion of the assessment, DHS shall make a determination if any changes to future DHS operations are required to address security vulnerabilities identified in such assessment.

*Mind Your Own Business Act of 2021;* S.1444 117th Congress; Sponsor: Sen. Wyden, Ron [D-OR]: This bill requires assessments, periodic reporting, and the development of an opt-out process for specified commercial entities that operate high-risk information systems or automated-decision systems, such as those that use artificial intelligence or machine learning. An automated-decision system or information system is considered high risk if it (1) raises security or privacy concerns; (2) involves the personal information of a significant number of people; or (3) systematically monitors a large, publicly-accessible physical location. An automated-decision system is also considered high risk if it (1) may contribute to inaccuracy, bias, or discrimination; or (2) facilitates decision-making about sensitive aspects of consumers’ lives by evaluating their behavior. Covered commercial entities must assess such high-risk systems and evaluate the extent to which they protect against the risk of exposing personal information. The bill further requires certain larger commercial entities to submit an annual report for which corporate officers must certify that the entity is in compliance with the Federal Trade Commission’s (FTC) implementing regulations. A failure to comply with the reporting requirements is subject to criminal penalties and excise tax.

*National Cyber Director Act;* H.R.7331 116th Congress; Sponsor: Rep. Langevin, James R. [D-RI-2]: This bill establishes the Office of the National Cyber Director, the duties of which shall include (1) serving as the principal advisor to the President on cybersecurity strategy and policy, (2) developing and supervising implementation of the U.S. National Cyber Strategy, and (3) directing the response of the federal government to cyberattacks and cyber campaigns of significant consequence.

*National Laboratory Biotechnology Research Act of 2021;* S.1624 117th Congress; Sponsor: Sen. Lujan, Ben Ray [D-NM]: This bill directs the Department of Energy (DOE) to establish a National Laboratory Biotechnology Program to integrate the resources of DOE, including the Office of Science, the Office of Intelligence and Counterintelligence, and the National Nuclear Security Administration, to provide research and development and response capabilities to respond to long-term biotechnology threats facing the United States, and any remaining threats posed by COVID-19. The Office of Science shall support research that harnesses the capabilities of the national laboratories to address advanced biological threats of national security significance.

*National Science-Based Education Campaign to Increase Public Awareness Regarding the Use of Technology in Food and Agriculture;* H.R.6386 115th Congress; Sponsor: Rep. Dunn, Neal P. [R-FL-2]: This bill directs the Department of Agriculture (USDA) to: carry out a national science-based education campaign to increase public awareness of the use of technology in food and agriculture production, and establish a federal government website through which the public may obtain information about biotechnology used in the food and agricultural sectors. USDA may use publicly available social media platforms in supplementing the national science-based education campaign and as an extension of such website.

*Next Generation Computing Research and Development Act of 2021;* H.R.3284 117th Congress; Sponsor: Rep. Obernolte, Jay [R-CA-8]: This bill provides for the support of advanced scientific computing programs and activities at the Department of Energy (DOE). The DOE Office of Science shall carry out a research and development program to advance computational and networking capabilities to analyze and predict complex phenomena relevant to the development of new energy technologies and U.S. competitiveness. DOE shall establish a program to implement a strate gy for achieving computing systems with capabilities beyond exascale computing systems; support a program of fundamental research and development of energy efficient computing technologies relevant to advanced computing applications in high performance computing, artificial intelligence, and scientific machine learning; and provide for an upgrade to the Energy Sciences Network user facility in order to meet federal research needs for highly reliable data transport capabilities optimized for the requirements of large-scale science.

*NIST COVID-19 Cybersecurity Act;* H.R.7998 116th Congress; Sponsor: Rep. Barr, Andy [R-KY-6]: This bill instructs the National Institute of Standards and Technology (NIST) to consider institutions of higher education when facilitating and supporting the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure. In using such authority, NIST shall disseminate and make publicly available resources to help research institutions and institutions of higher education identify, assess, manage, and reduce their cybersecurity risk related to conducting research with respect to COVID-19 (coronavirus disease 2019).

*Reporting Attacks from Nations Selected for Oversight and Monitoring Web Attacks and Ransomware from Enemies Act or the RANSOMWARE Act;* H.R.4551 117th Congress; Sponsor: Rep. Bilirakis, Gus M. [R-FL-12]: This bill requires the Federal Trade Commission to report on cross-border complaints received that involve ransomware or other cyber-related attacks committed by certain foreign individuals, companies, and governments. The report must focus specifically on attacks committed by (1) Russia, China, North Korea, or Iran; or (2) individuals or companies that are located in or have ties to those countries.

*Risk-Informed Spending for Cybersecurity Act;* S.4785 116th Congress; Sponsor: Sen. Portman, Rob [R-OH]: This bill requires the Office of Management and Budget, in coordination with the Cybersecurity and Infrastructure Security Agency, to develop a standard model for creating a risk-based budget for cybersecurity spending. The risk-based budget must (1) be developed by identifying and prioritizing cybersecurity risks and vulnerabilities through analysis of threat intelligence, incident data, and tactics, techniques, procedures, and capabilities of cyber threats; and (2) allocate resources based on the risks identified and prioritized. Within two years of the development of the model, federal agencies must begin using the model to develop annual cybersecurity and information technology budget requests.

*Satellite Cybersecurity Act;* S.3511 117th Congress; Sponsor: Peter, Gary [D-MI]: This bill addresses cybersecurity matters related to commercial satellite systems. Specifically, the Cybersecurity and Infrastructure Security Agency (CISA) must maintain a publicly available clearinghouse of resources concerning the cybersecurity of commercial satellite systems. CISA must also develop voluntary recommendations for the development, maintenance, and operation of such systems. The recommendations must include measures to protect systems against cyber-related vulnerabilities, risks, and attacks. The bill also requires the Government Accountability Office (GAO) to study and report on federal actions to support the cybersecurity of commercial satellite systems, including with respect to critical infrastructure sectors. In carrying out its study and report, the GAO must coordinate with designated federal agencies.

*SBA Cyber Awareness Act;* H.R.3462 117th Congress; Sponsor: This bill requires the Small Business Administration (SBA) to annually report specified information related to cybersecurity awareness. Such reports must provide (1) an assessment of the SBA’s information technology (IT) and cybersecurity infrastructure, (2) a strategy to increase such infrastructure, (3) a detailed account of the SBA’s IT equipment that is manufactured by an entity that has its principal place of business in China, and (4) any SBA cybersecurity risk or incident that occurred during the two years prior to the report (including the SBA’s action to respond to or remediate it).

*Securing American Research From Cyber Theft Act;* H.R.3747 117th Congress; Sponsor: Rep. Babin, Brian [R-TX-36]: This bill establishes a pilot program and modifies a current program related to cybersecurity for federally supported research and data. The bill directs the National Science Foundation to award grants to establish a pilot program to ensure the security of federally supported research data and to assist regional institutions of higher education and their researchers in complying with regulations regarding the safeguarding of sensitive information and other relevant regulations and federal guidelines. The bill requires the Networking and Information Technology Research and Development Program to provide for improving the security, reliability, and resiliency of computing and networking systems used by higher education and other nonprofit research institutions for the processing, storage, and transmission of sensitive federally funded research and associated data.

*Small Business Development Center Cyber Training Act of 2021;* H.R.4515 117th Congress; Sponsor: Rep. Garbarino, Andrew R. [R-NY-2]: This bill requires the Small Business Administration to establish a program for certifying at least 5 or 10% of the total number of employees of a small business development center to provide cybersecurity planning assistance to small businesses.

*Space Infrastructure Act;* H.R.3713 117th Congress; Sponsor: Rep. Lieu, Ted [D-CA-33]: This bill directs the Department of Homeland Security to designate space systems, services, and technology as a critical infrastructure sector. Under current law, critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

*State and Local Government Cybersecurity Act of 2021;* H.R.5960 117th Congress; Sponsor: Rep. Neguse, Joe [D-CO-2]: This bill provides for collaboration between the Department of Homeland Security (DHS) and state, local, tribal, and territorial governments, as well as corporations, associations, and the general public, regarding cybersecurity. The bill expands DHS responsibilities through grants and cooperative agreements, including provision of assistance and education related to cyber threat indicators, defensive measures, cybersecurity risks or vulnerabilities, and incident response and management. The bill requires the National Cybersecurity and Communications Integration Center, upon request, to coordinate with entities such as the Multi-State Information Sharing and Analysis Center to engage in specified activities, including to (1) conduct exercises with state, local, tribal, or territorial government entities; (2) provide operational and technical cybersecurity training to such entities; and (3) promote cybersecurity education and awareness.

*State Cyber Resiliency Act;* H.R.4910 117th Congress; Sponsor: Rep. Kilmer, Derek [DWA-6]: This bill establishes the State Cyber Resiliency Grant Program to assist state, local, and tribal governments in preventing, preparing for, protecting against, and responding to cyber threats. Under this program, the Department of Homeland Security may award grants to a state for the development and implementation of an active cyber resiliency plan. Such plan must be tailored to achieve specific objectives, including enhancement of the response and resiliency of computer networks, industrial control systems, and communications systems against cybersecurity threats or vulnerabilities; implementation of continuous vulnerability assessments and threat mitigation practices; adoption of cybersecurity best practices by entities performing cybersecurity functions within a state; and confirmation that continuity of communications and data networks would be maintained in the event of a catastrophic disruption of such communications or networks.

*Strengthening American Cybersecurity Act of 2022;* S.3600 117th Congress; Sponsor: Peters, Gary C. [D-MI]: This bill addresses cybersecurity threats against critical infrastructure and the federal government. The Cybersecurity and Infrastructure Security Agency (CISA) must perform ongoing and continuous assessments of federal risk posture. An agency, within a specified time frame, must (1) determine whether notice to any individual potentially affected by a breach is appropriate based on a risk assessment; and (2) as appropriate, provide written notice to each individual potentially affected. Each agency must (1) provide information relating to a major incident to specified parties, and (2) develop specified training for individuals with access to federal information or information systems. The bill requires reporting and other actions to address cybersecurity incidents. Entities that own or operate critical infrastructure must report cyber incidents and ransom payments within specified time frames. The bill limits the use and disclosure of reported information. The bill establishes (1) an interagency council to standardize federal reporting of cybersecurity threats, (2) a task force on ransomware attacks, and (3) a pilot program to identify information systems vulnerable to such attacks.

*Strengthening the Cybersecurity and Infrastructure Security Agency Act of 2020;* H.R.7588 116th Congress; Sponsor: Rep. Katko, John [R-NY-24]: This bill directs the Cybersecurity and Infrastructure Security Agency (CISA) and the General Services Administration (GSA) to carry out specified reviews related to the ability of CISA to carry out its mission. Specifically, CISA must undertake a review that includes an assessment of (1) how additional budget resources could be used for certain projects, (2) whether existing personnel are appropriately matched to the prioritization of threats in the cyber domain and risks to critical infrastructure, and (3) its facilities and their suitability to support current and projected mission requirements. Additionally, the GSA must review CISA’s assessment of its facilities and make recommendations regarding necessary resources for procuring or building new or augmented facilities.

*Study on Cyber-Attack Response Options Act;* S.2292 117th Congress; Sponsor: Sen. Daines, Steve [R-MT]: This bill directs the Department of Homeland Security to study and report on the potential benefits and risks of amending the federal statute commonly known as the Computer Fraud and Abuse Act to allow private entities to respond to an unlawful network breach, subject to federal regulation and oversight. The Computer Fraud and Abuse Act prohibits various categories of computer-related conduct by an individual without authority or in excess of authorization.